Avocent

SwitchView® IP 1020
Remote Access Device

Installer/User Guide

USA Notification

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Canadian Notification

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Japanese Notification

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Korean Notification

기종별	사용자 안내문
A급 기기 (업무용 정보통신기기)	이기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 구입 하였을 때에는 가정용으로 교환하시기 바랍니다.

Safety and EMC Approvals and Markings

UL, FCC, cUL, ICES-003, CE, GS, VCCI, MIC, C-Tick

SwitchView® IP 1020 Remote Access Device

Installer/User Guide

Instructions

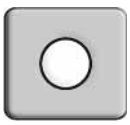
This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Power On

This symbol indicates the principal on/off switch is in the on position.



Power Off

This symbol indicates the principal on/off switch is in the off position.

Protective Grounding Terminal

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Product Overview

Features and Benefits

The Avocent SwitchView® IP 1020 remote access device combines analog and digital technology to provide flexible control of data center servers, and to facilitate the OA&M (operations, activation and maintenance) of remote branch offices where trained operators may be unavailable. The remote access device provides our customers with a significant reduction of cable volume, secure remote access and flexible server management from anywhere at anytime.

The SwitchView IP 1020 device is a keyboard, video and mouse (KVM) remote access device configurable for analog (local) or digital (remote) connectivity. Video resolutions up to 1280 x 1024 are supported for remote users. Enhanced video quality of up to 1600 x 1200 is available to local users via the video port.

The IP-based SwitchView IP 1020 remote access device gives you flexible target device management control from anywhere in the world.

Accessing a remote access device via network connection

No special software or drivers are required on the attached, or client, computers. Users access the SwitchView IP 1020 remote access device and an attached system via the Ethernet from a client computer, such as a PC. Clients can be located anywhere a valid network connection exists. Both IPv4 (default) or IPv6 modes are supported.

Simple access to a target device

When a user selects the target device, the video of the selected target device is displayed in a Video Viewer window.

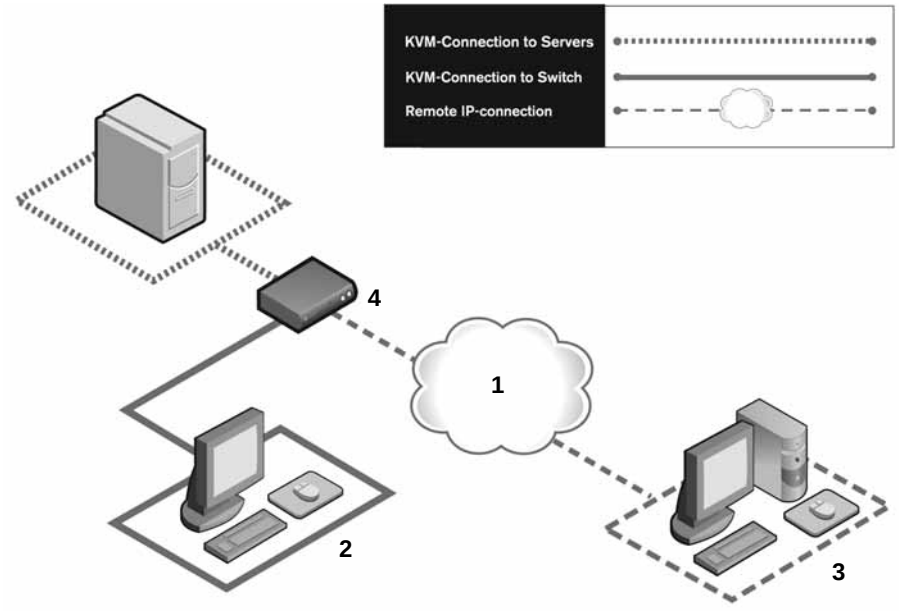


Figure 1.1: Example SwitchView IP 1020 Remote Access Device Configuration

Table 1.1: Descriptions for Figure 1.1

Number	Description
1	Ethernet
2	Analog User
3	Digital User (Computer with Internet browser)
4	SwitchView IP 1020 Remote Access Device

CHAPTER 2

Installation

SwitchView IP 1020 Remote Access Device Connectivity

The SwitchView IP 1020 remote access device transmits keyboard, video and mouse (KVM) information between operators and a target device attached to the remote access device over a network using an Ethernet connection.

The SwitchView IP 1020 remote access device uses TCP/IP for communication over Ethernet. You can access and control your target device with GUI-based simplicity using the built-in web server.

Installation Overview

The general procedure for setting up and installing a SwitchView IP 1020 remote access device is as follows:

- Unpack the switch and verify that all components are present and in good condition.
- Make all hardware connections between the power source, remote access device, target device and the Ethernet connection.
- Turn on the power and verify that all connections are working.
- Make the appropriate mouse setting adjustments.

Figure 2.1 illustrates a basic configuration for the SwitchView IP 1020 remote access device, using the SwitchView IP 1020 model for the example. Descriptions follow in Table 2.1.

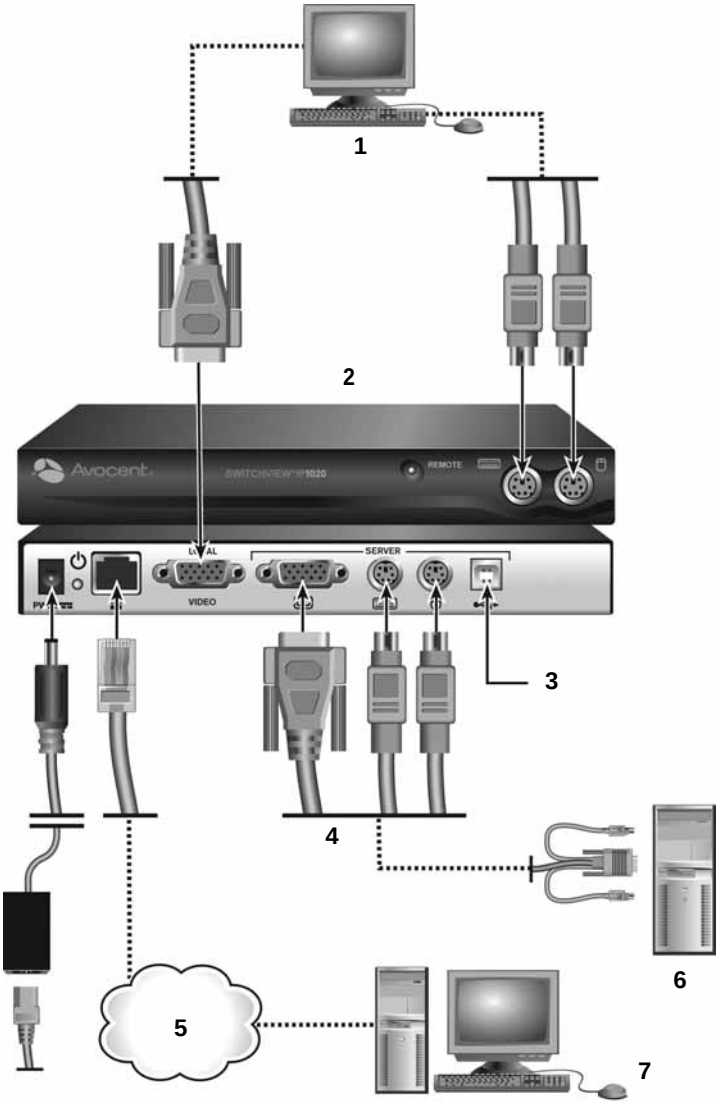


Figure 2.1: Basic SwitchView IP 1020 Remote Access Device Configuration

Table 2.1: Descriptions for Figure 2.1

Number	Description	Number	Description
1	Local User	**5**	Ethernet
2	SwitchView IP 1020 Remote Access Device	6	Server
3	Optional USB Port	**7**	Remote User
4	CPS2-6A Cable		

Getting started

Before installing your SwitchView IP 1020 remote access device, refer to the following lists to ensure you have all items that shipped with the SwitchView IP 1020 remote access device, as well as other items necessary for proper installation.

Supplied with the SwitchView IP 1020 remote access device

- Power adaptor
- Power cord
- Avocent CPS2-6A cable
- SwitchView IP 1020 Remote Access Device Quick Installation Guide

Additional items needed

- One CAT5 patch cable for network connectivity (4 pair UTP)

Setting up your network

The SwitchView IP 1020 remote access device system uses IP addresses to uniquely identify the switch and the target device. The SwitchView IP 1020 remote access device family supports both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Avocent recommends that IP addresses be reserved for each SwitchView IP 1020 remote access device and that they remain static while the switches are connected to the network.

Connecting the Remote Access Device Hardware

To connect and power your SwitchView IP 1020 remote access device:

1. Power down the target server that will be attached to your SwitchView IP 1020 remote access device. Locate the power adaptor and cord that came with your remote access device. Plug the barrel connector into the back panel of the SwitchView IP 1020 device, the AC power cord into the adaptor block and the AC connector into an appropriate AC wall outlet.

WARNING: The power cord is considered the main disconnect device.

2. To connect a local user, plug a VGA monitor into the port labeled LOCAL VIDEO on the back panel of the remote access device. Plug the PS/2 keyboard and mouse cables into the appropriately labeled ports located on the front of the remote access device.
3. To connect to the server, plug one end of the CPS2-6A cable into the server's VGA, keyboard and mouse ports. Plug the other end into the SERVER VGA, keyboard and mouse ports on the back panel of the SwitchView IP 1020 remote access device.

NOTE: If using USB keyboard and mouse peripherals, plug one end of a USB cable into the server and the other end into the optional USB port on the SwitchView IP 1020 device. Disconnect the PS/2 connectors of the CPS2-6A cable from the server, if applicable.

4. Plug a CAT 5 patch cable from your Ethernet network into the LAN port on the back of the SwitchView IP 1020 remote access device.
5. Power up the target device and then the SwitchView IP 1020 remote access device. After approximately one minute, the device will complete initialization and display video on the local port monitor.
6. Point your web browser to the default IP address https://192.168.1.254 to access the device.
7. Log in to the SVIP1020 Explorer window and, using the top menu bar, select *Appliance-Appliance Settings-Network.* Enter the appropriate addressing information for your network.

NOTE: The default username is Admin with no password.

SwitchView IP 1020 remote access device LEDs

The front panel of the SwitchView IP 1020 remote access device features a blue LED that indicates remote connection. On the back panel of the device, a green LED indicates power. If the power LED blinks continuously, the device is in recovery mode.

Also, on the back panel of the device, the two LEDs for the LAN connector do the following:

- Illuminates green when a valid connection to the network is established and blinks when there is activity on the port

Illuminates amber to indicate that you are communicating at the 100 Mbps rate when using an Ethernet connection

Adjusting Mouse Settings on Target Devices

Before a computer connected to the SwitchView IP 1020 remote access device can be used for remote user control, you must set the target mouse speed and turn off acceleration. For machines running Microsoft® Windows® (Windows NT®, 2000, XP, Server 2003), use the default PS/2 mouse driver.

To ensure that the local mouse movement and remote cursor display remain in sync, mouse acceleration must be set to “none” for all user accounts accessing the target computer with the SwitchView IP 1020 remote access device. Mouse acceleration must also be set to “none” on every remote system. Special cursors should not be used and cursor visibility options, such as pointer trails, **Ctrl** key cursor location animations, cursor shadowing and cursor hiding, should also be turned off.

CHAPTER 3

Web Interface Operations

On-Board Web Interface

The SwitchView IP 1020 remote access device provides an on-board web interface to manage remote access. The remote access device on-board web interface provides secure “point-and-click” web browser-based access to control any device attached to your SwitchView IP 1020 remote access device.

Table 3.1 shows which operating systems and browsers the SwitchView IP 1020 remote access device on-board web interface supports.

Table 3.1: On-Board Web Interface Supported Operating Systems and Browsers

	Browser		
Operating System	**Microsoft® Internet Explorer version 6.0 SP1 and later**	**Mozilla version 1.7.3 and later**	**Firefox version 1.0 and later**
Windows 2000 Workstation or Server with Service Pack 2	Yes	Yes	Yes
Windows Server 2003 Standard, Enterprise or Web Edition	Yes	Yes	Yes
Windows XP Home Edition or Professional	Yes	Yes	Yes
Red Hat Enterprise Linux 3 and 4	No	Yes	Yes
Sun Solaris 9 and 10	No	Yes	Yes
Novell SUSE® Linux Enterprise 9 and 10	No	Yes	Yes
Fedora Core 4 and 5	No	Yes	Yes
Mac OS X Tiger (10.4+)	No	No	Yes

NOTE: Mac OS X requires Firefox 1.5 or later.

Avocent recommends that the browser be kept up-to-date with the latest version.

A Video Viewer window allows you to control the keyboard, monitor and mouse functions of individual target devices connected to the SwitchView IP 1020 remote access device in real time. You may also use predefined global macros to perform actions within the Video Viewer window. For instructions on how to use the Video Viewer, see Chapter 4. Once the switch has been installed and configured as described in Chapter 2 and you have set the IP address, you are ready to begin regular operation.

Logging into the SwitchView IP 1020 remote access device

NOTE: The SwitchView IP 1020 remote access device boots to the following static IP address, gateway and netmask:
IP address: 192.168.1.254
Gateway: 192.168.1.1
Netmask: 255.255.255.0

Before you can begin a KVM session, you must first login to the SwitchView IP 1020 remote access device on-board web interface.

To log into the SwitchView IP 1020 remote access device on-board web interface:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address or host name assigned to the SwitchView IP 1020 remote access device you wish to access. Use https://xxx.xx.xx.xx or https://hostname as the format.
3. When the browser makes contact with the switch, enter your username and password, then click *Login*. The SwitchView IP 1020 Explorer Window will appear.

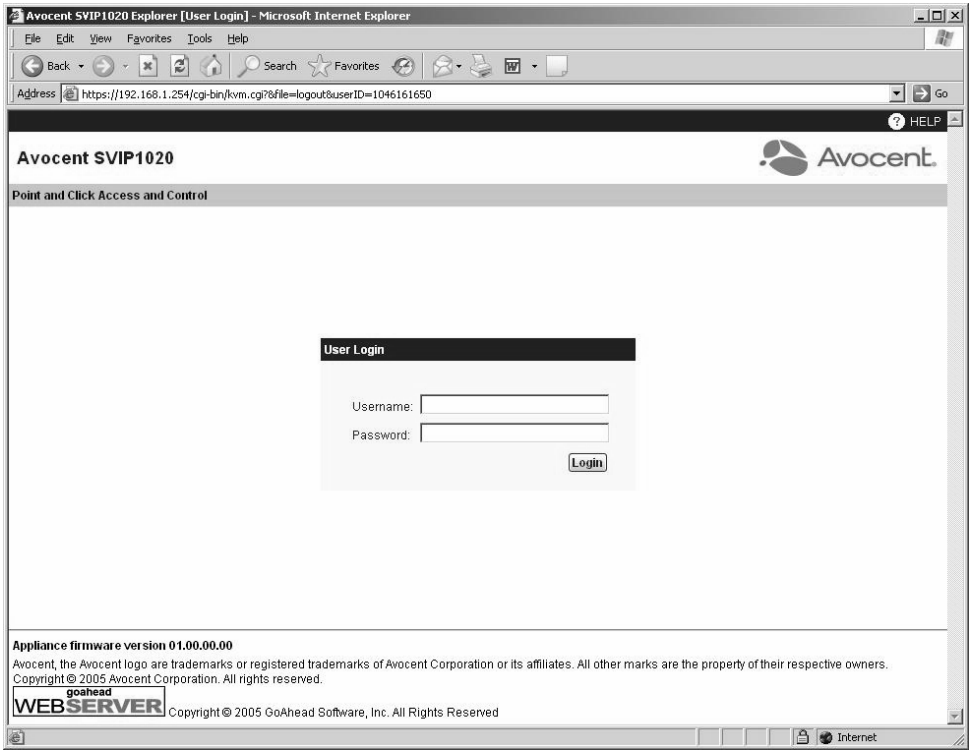


Figure 3.1: SVIP 1020 Explorer (User Login) Screen

NOTE: The default username is Admin with no password.

The SwitchView IP 1020 Explorer Window

When a user has been logged in and authenticated, the Avocent SwitchView IP 1020 Explorer window appears. From the SwitchView IP 1020 Explorer window, users may view, access and manage their SwitchView IP 1020 remote access device. The window may also be used to specify system settings and change profile settings.

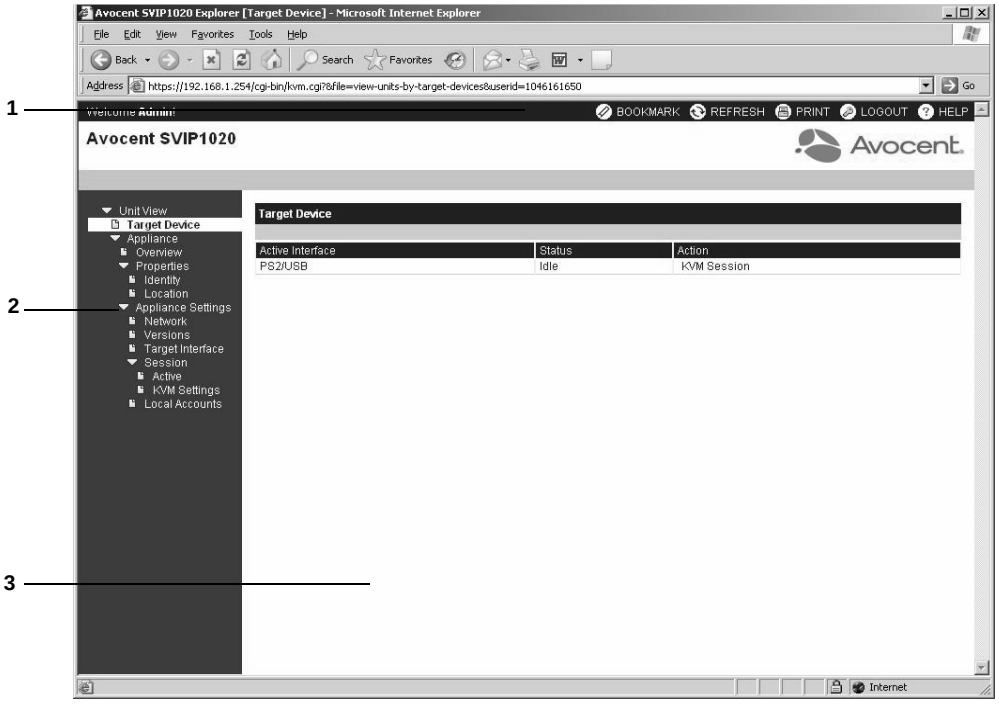


Figure 3.2: Avocent SwitchView IP 1020 Explorer Window

Table 3.2: Descriptions for Figure 3.2

Number	Description
1	Top option bar: Use the top option bar to bookmark a SwitchView IP 1020 remote access device on-board web interface window, refresh the display of a SwitchView IP 1020 remote access device on-board web interface window, print a web page, log out of a software session or access the Avocent Technical Support help page. The name of the logged in user appears on the left side of the top option bar.
2	Side navigation bar: Use the side navigation bar to display the system information you wish to display or edit, which displays in the content area. The side navigation bar also contains icons in the top left corner which, when clicked, expand or collapse all nodes.
3	Content area: Use the content area to display or make changes to the SwitchView IP 1020 remote access device on-board web interface system.

Using the side navigation bar

You can use the side navigation bar to display windows in which you can specify settings or perform operations. Clicking on a link that does not contain an arrow will display its corresponding window.

Using the top option bar

Bookmarking a window

The SwitchView IP 1020 Explorer window contains a bookmark icon and text in the top option bar. Bookmarking a window will add a link to the window in the Favorites drop-down menu. You may select the link at any time to quickly access the bookmarked window.

If you bookmark a window and information related to the window changes, this new information will appear in the window when you next display the bookmarked window.

If you click *BOOKMARK* or the bookmark icon after the SwitchView IP 1020 remote access device on-board web interface session has timed out, the User Login window will open and you must log in again.

To bookmark a window:

1. In the top option bar, click *BOOKMARK* or the bookmark icon. The Add Favorite dialog box will appear.
2. If you wish, type a name for the window. You may also click the *Create in* button to create or specify a folder in which to place the window.
3. Click *OK* to close the Add Favorite dialog box.

Printing a window

All SwitchView IP 1020 remote access device on-board web interface windows contain a print icon in the top option bar.

To print a SwitchView IP 1020 remote access device on-board web interface window:

1. In the top option bar, click *PRINT* or the print icon. The Print dialog box will appear.
2. Specify the options you wish to use for printing the SwitchView IP 1020 remote access device on-board web interface window.
3. Click *Print* to print the SwitchView IP 1020 remote access device on-board web interface window and close the Print dialog box.

Refreshing a window

The SwitchView IP 1020 Explorer window may be refreshed at any time by clicking *REFRESH* or the refresh icon in the top option bar.

Logging out

A user may log out at any time by clicking the logout icon in the top option bar.

Managing local accounts

The remote access device web interface provides local and login security through Administrator-defined user accounts. By selecting *Local Accounts* on the side menu bar, Administrators may add and delete users, define user preemption and access levels and change passwords.

User access levels

Accounts have two access levels: user and administrator. Most switch management tasks can only be performed by persons with administrator level access.

Preemption levels

The preemption level of users determine whether they may disconnect another user's serial or video (KVM) session with a target device.

Remote access device web interface administrators may specify the preemption level for user accounts when an account is created. The preemption level may be changed later.

Preemption levels range from 1-4, with 4 being the highest level. For example, a user with a preemption level of 4 may preempt other level 4 users, as well as those with a level 1, 2 or 3 setting.

To add a new user account (Administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the *Add* button.
3. Enter the name and password of the new user in the blanks provided.
4. Select the preemption and access levels for the new user.
5. Click the *Save* button to complete the process.

To delete a user account (Administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the box to the left of each account that you wish to delete, then click the delete button.

To edit a user account (Administrator or active user only):

1. On the side menu bar, select local accounts. The current user list will be displayed.
2. Click the name of the user you wish to edit. A user profile will appear.
3. Edit the user account as needed, then click *Save*.

Managing device properties

Viewing and changing appliance configuration information

The SwitchView IP 1020 remote access device can report most device properties directly through the remote access device web browser.

NOTE: Users can view all appliance information, but only Administrators can change settings.

Table 3.3: Viewing Appliance Information

To do this:	Select this:
Display the unit's name or type	*Appliance - Overview*
Display a list of available target devices, their type and status	*Target Devices*
Enter, change or display the unit's IP version, network address, gateway address, subnet mask, MAC address, LAN speed, DHCP enable status or ICMP ping reply status	*Appliance - Appliance Settings - Network* **NOTE:** If DHCP is set to Enabled before changing the IP mode to either IPv4 or IPv6, the user should also verify that the DHCP server has a predetermined IP address associated with the MAC address of the remote access device.
Display the unit's current firmware revision for application, boot and Video FPGA	*Appliance - Appliance Settings - Versions*
Display a list of active KVM sessions and their duration	*Appliance - Appliance Settings - Sessions - Active*
View the unit's part number, serial number and EID number	*Appliance - Properties - Identity*
Enter or display the unit's Site, Department and Location	*Appliance - Properties - Location*
Enable the inactivity timeout	*Appliance - Appliance Settings - Sessions - KVM settings* Then, click the *Enable Inactivity timeout* box.
Change the unit encryption level	*Appliance - Appliance Settings - Sessions - KVM settings* Then select the level of encryption desired for keyboard/ mouse signals and then video signals.

Configuring LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy and integrity.

If individual user accounts are stored on an LDAP-enabled directory service, such as Active Directory, you can use the directory service to authenticate users. The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the OBWI let you configure your authentication configuration parameters. The software sends the username, password and other information to the appliance, which then determines whether the user has permission to view or change configuration parameters for the appliance in the OBWI.

NOTE: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values may cause LDAP authentication server communication errors.

LDAP Overview parameters

On the LDAP Overview page in the OBWI, you can configure the LDAP authentication priority and the parameters that define LDAP server connection information.

LDAP authentication priority

In the LDAP Priority section of the LDAP Overview page, you can disable LDAP, or you can set the authentication priority by choosing whether local authentication or LDAP authentication should happen first.

To configure LDAP authentication priority parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.*
2. Select either *LDAP Disabled*, *LDAP before Local* or *LDAP after Local* for the LDAP Priority.
3. Click *Save*.

LDAP servers

The Address fields specify the host names or IP addresses of the primary and secondary LDAP servers. The second LDAP server is optional.

The Port fields specify the User Datagram Protocol (UDP) port numbers that communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP (LDAPS). The default Port ID is automatically entered by the software when an access type is specified.

The Access Type radio buttons specify how a query is sent to each LDAP target device. When using LDAP, all usernames, passwords and other information sent between an appliance and LDAP server are sent as non-secure clear text. Use LDAPS for secure encrypted communication between an appliance and LDAP server.

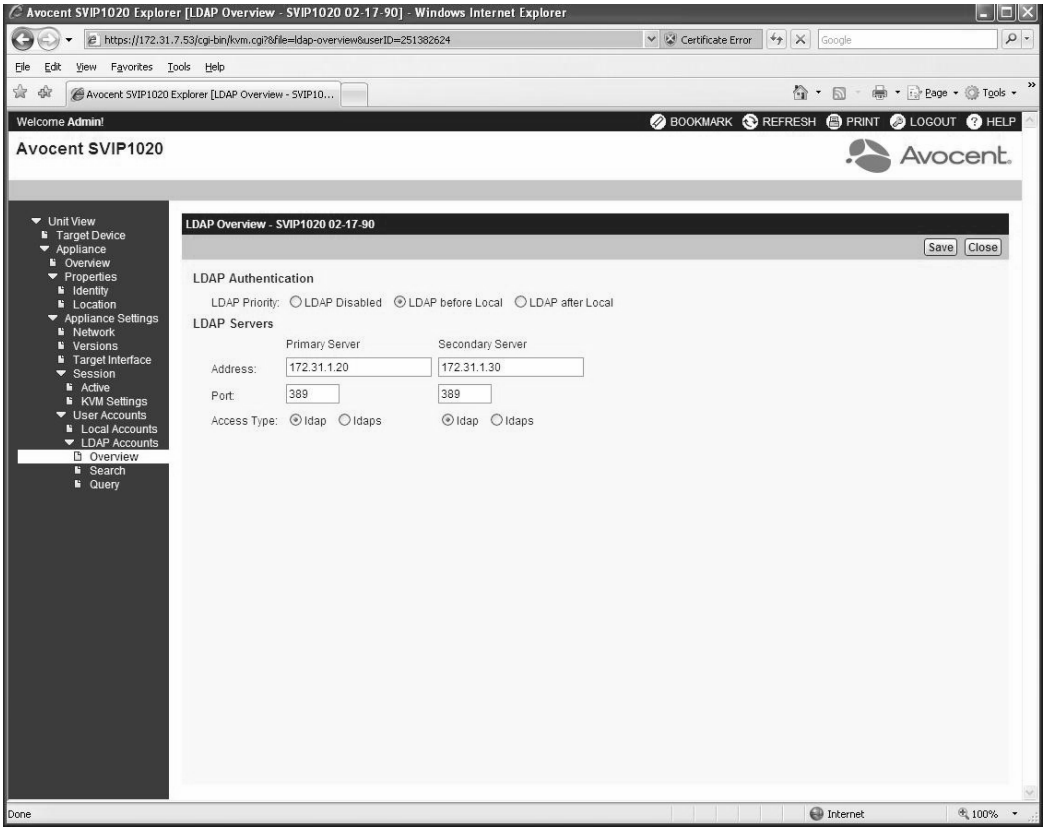


Figure 3.3: LDAP Overview Page in the OBWI

To configure LDAP server parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Overview.*
2. Identify the primary and secondary server address, port and access type in the appropriate fields or radio buttons.
3. Click *Save*.

LDAP Search parameters

On the LDAP Search page, you can configure the parameters used when searching for LDAP directory service users.

Use the Search DN field to define an administrator-level user that the appliance uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the Query page. The default values are cn=Administrator, cn=Users, dc=yourDomainName and dc=com and may be modified. For

example, to define an administrator Distinguished Name (DN) for test.view.com, type **cn=Administrator, cn=Users, dc=test, dc=view,** and **dc=com.** This Search DN field is a required field unless the directory service has been configured to enable anonymous search, which is not the default. Each Search DN value must be separated by a comma.

The Search Password field is used to authenticate the administrator or user specified in the Search DN field.

Use the Search Base field to define a starting point from which LDAP searches begin. The modifiable default values are dc=yourDomainName and dc=com. For example, to define a search base for test.com, type **dc=test, dc=com**. Each Search Base value must be separated by a comma.

The UID Mask field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form <name>=<%1>. The default value is sAMAccountName=%1, which is correct for use with Active Directory. This field is required for LDAP searches.

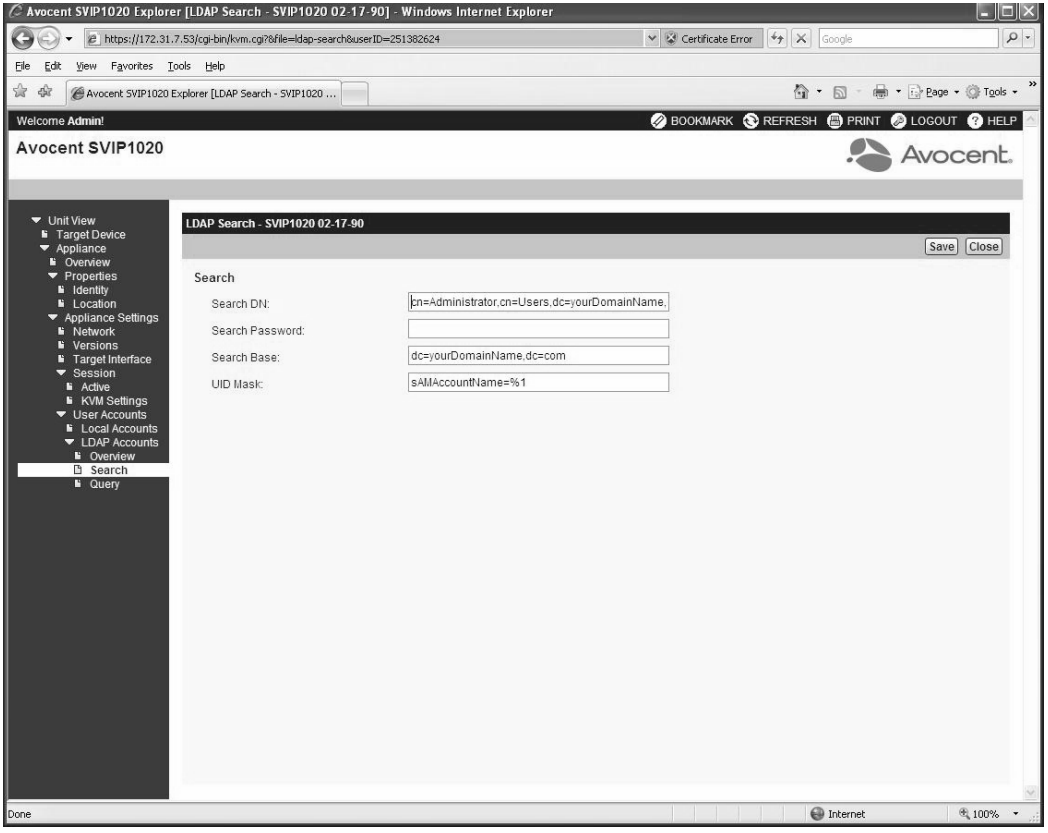


Figure 3.4: LDAP Search Page in the OBWI

To configure LDAP search parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Search*.
2. Enter the appropriate information in the Search DN, Search Password, Search Base and UID Mask fields.
3. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

LDAP Query parameters

On the LDAP Query page, you can configure the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query Mode (Appliance) is used to authenticate administrators attempting to access the appliance itself. Query Mode (Target Device) is used to authenticate users that are attempting to access attached target devices. Additionally, each type of query has three modes that utilize certain types of information to determine whether or not a VCS user has access to an appliance or connected target devices. See *Appliance and Target Device Query Modes* on page 21 for detailed information on each mode.

You can configure the following settings on the LDAP Query page:

- The Query Mode (Appliance) parameters determine whether or not a user has access to the appliance.
- The Query Mode (Target Device) parameters determine whether or not a user has user access to target devices connected to an appliance. The user does not have access to the appliance.
- The Group Container, Group Container Mask and Target Mask fields are only used for group query modes and are required when performing an appliance or device query.
- The Group Container field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects. Group objects are Active Directory objects that can contain users, computers, contacts and other groups. Group Container is used when Query Mode is set to Group Attribute. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object. For example, if the Notes property in the group object is used to implement the access control attribute, the Access Control Attribute field on the LDAP Query page should be set to info. Setting the Notes property to KVM User Admin causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.
- The Notes property is used to implement the access control attribute. The value of the Notes property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the info attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by

selecting *Start - Programs - Administrative Tools -Active Directory Users and Computers*. This tool is used to create, configure and delete objects such as users, computers and groups.

- The Group Container Mask field defines the object type of the Group Container, which is normally an organizational unit. The default value is “ou=%1”.
- The Target Mask field defines a search filter for the target device. The default value is “cn=%1”.
- The Access Control Attribute field specifies the name of the attribute that is used when the query modes are set to Attribute. The default value is info.

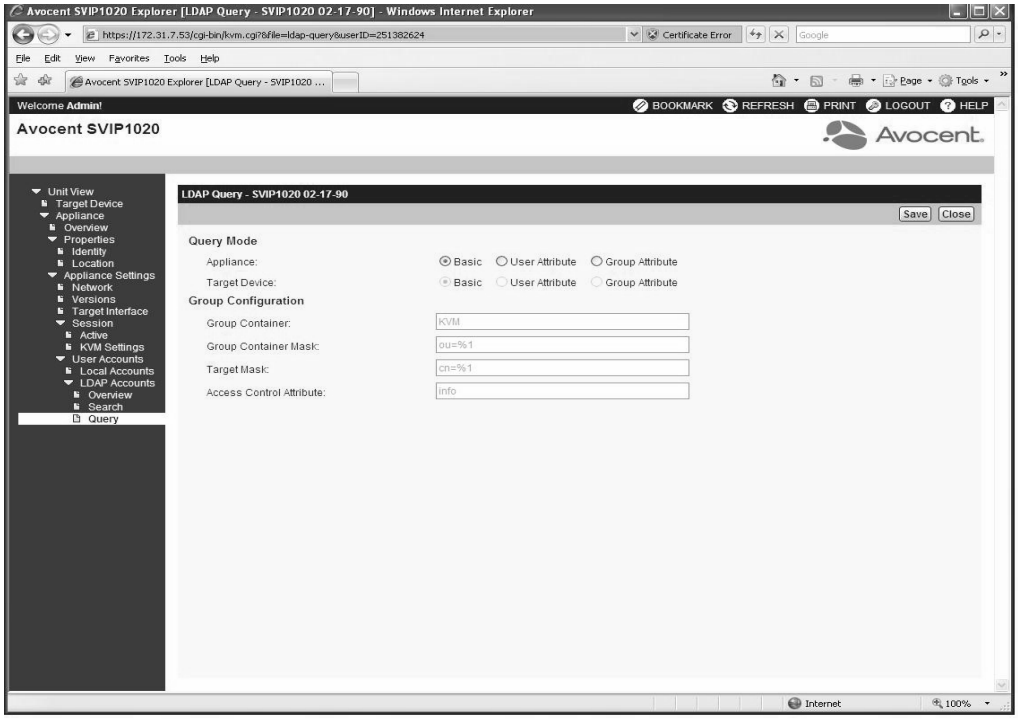


Figure 3.5: LDAP Query Page in the OBWI

To configure LDAP query parameters:

1. Select *Appliance - Appliance Settings - User Accounts - LDAP Accounts - Query.*
2. Select either *Basic*, *User Attribute* or *Group Attribute* for the Appliance Query Mode and the Target Device Query Mode.
3. Enter the appropriate information in the Group Container, Group Container Mask, Target Mask and Access Control Attribute fields.
4. Click *Save*.

NOTE: These options cannot be changed if the LDAP Priority is set to *LDAP Disabled* on the Overview screen.

Appliance and Target Device Query Modes

One of three different modes can each be used for Query Mode (Appliance) and Query Mode (Target Device):

- Basic – A username and password query for the user is made to the directory service. If they are verified, the user is given administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).
- User Attribute – A username, password and Access Control Attribute query for the appliance user is made to the directory service. The Access Control Attribute is read from the user object (the user account) in Active Directory.

  If the KVM Appliance Admin value is found, the user is given appliance administrator access to the appliance and any attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device). If the KVM User Admin value is found, the user is given User administrator access to the appliance and attached target devices for Query Mode (Appliance), or to any selected target device for Query Mode (Target Device).

  The following are examples showing how the KVM Appliance Admin and KVM User Admin attribute modes are defined in Active Directory for a user named John Smith, stored in the ADUC. You can access the ADUC by selecting *Start - Programs - Administrative Tools - Active Directory Users and Computers*.

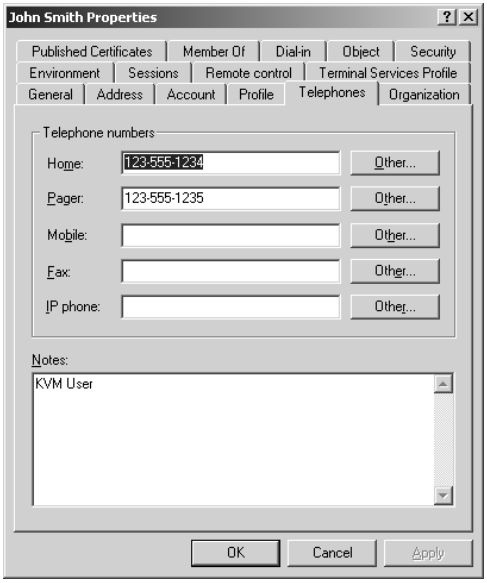


Figure 3.6: Active Directory - KVM User

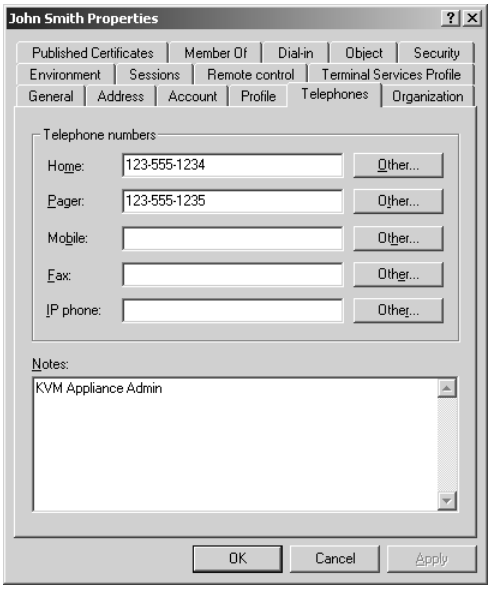


Figure 3.7: Active Directory - KVM Appliance Admin

- Group Attribute – A username, password and group query is made to the directory service for an appliance and attached target devices when using Query Mode (Appliance), or for a selected target device when using Query Mode (Target Device). If a group is found containing the user and the appliance name, the user is given access to the appliance or attached target devices, depending on the group contents, when using Query Mode (Appliance). If a group is found containing the user and target device IDs, the user is given access to the selected target device connected to the appliance when using Query Mode (Target Device).

  Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you may have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group may contain a member named Domestic, which is a group, and so on.

  The following is an example of groups defined in Active Directory.

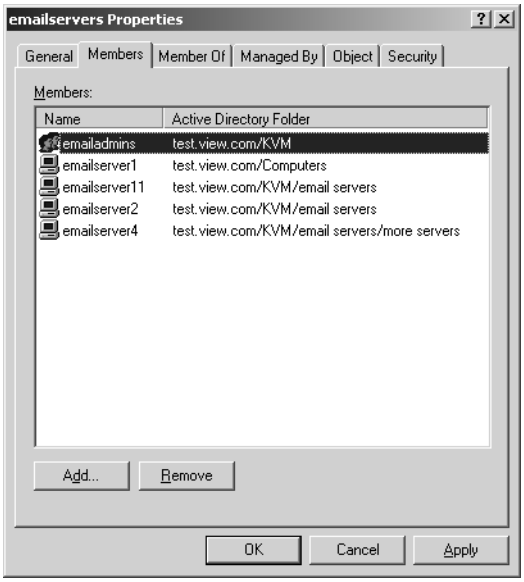


Figure 3.8: Active Directory - Define Groups

Setting up Active Directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the user.

To set up group queries:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create an object in Active Directory with a name identical to the switching system name for querying appliances (specified in the Appliance Overview screen of the OBWI), or identical to the attached target devices for querying target devices. The name must match exactly, including case.
5. The appliance names and target device names used for group queries are stored in the appliance. The appliance name specified in the Appliance Overview screen of the OBWI and target device names must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints.

NOTE: The factory default name in earlier versions contains a space that must be removed by editing the switching system name in the Appliance Overview screen of the OBWI.

6. Create one or more groups under the group container organizational unit.
7. Add the usernames and target device and appliance objects to the groups you created in step 5.

Specify the value of any attribute being used to implement the access control attribute. For example, if you are using info as the attribute in the Access Control Attribute field and using the Notes property in the group object to implement the access control attribute, the value of the Notes attribute in Active Directory may be set to one of the three available access levels (KVM User, KVM User Admin or KVM Appliance Admin) for the group object. The members of the group may then access the appliances and target devices at the specified access level.

Rebooting the appliance

Periodically, such as after an upgrade, you may need to reboot the SwitchView IP 1020 remote access device.

To reboot the SwitchView IP 1020 remote access device remotely:

1. From the side navigation bar, select *Appliance - Overview.*
2. When the appliance overview window appears, click *Tools - Reboot Appliance*.

Managing local accounts

The SwitchView IP 1020 remote access device on-board web interface provides local and login security through administrator-defined user accounts. By selecting *Local Accounts* on the side menu bar, administrators may add and delete users, define user preemption and access levels and change passwords.

Access levels

When a user account is added to the on-board web interface, the user may be assigned to any of the following access levels:

- Appliance administrators
- User administrators
- Users

Table 3.4: Allowed Operations by Access Level

	Access Level		
Operation	**Appliance Administrator**	**User Administrator**	**Users**
Configure on-board web interface system-level settings	Yes	No	No
Configure access rights	Yes	Yes	No
Add, change and delete user accounts	Yes, for all access levels	Yes, for users and user administrators only	No
Change your own password	Yes	Yes	Yes
Access target device	Yes, all target devices	Yes, all target devices	Yes, if allowed

To add a new user account (administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the *Add* button.
3. Enter the name and password of the new user in the blanks provided.
4. Select the preemption and access levels for the new user.
5. Click the *Save* button to complete the process.

To delete a user account (administrator only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the box to the left of each account that you wish to delete, then click the *Delete* button.

To edit a user account (administrator or active user only):

1. On the side menu bar, select *Local Accounts*. The current user list will be displayed.
2. Click the name of the user you wish to edit. A user profile will appear.
3. Edit the user account as needed, then click *Save*.

Preemption levels

The preemption level of users determines whether they may disconnect another user's serial or video (KVM) session with a target device.

SwitchView IP 1020 remote access device on-board web interface administrators may specify the preemption level for user accounts when an account is created. Preemption levels range from 1-4,

with 4 being the highest level. For example, a user with a preemption level of 4 may preempt other level 4 users, as well as those with a level 1, 2 or 3 setting.

CHAPTER 4

The Video Viewer

The Video Viewer Window

The Video Viewer is used to conduct a KVM session with the target device attached to a SwitchView IP 1020 remote access device. When you connect to a device using the Video Viewer, the target device desktop appears in a separate window containing both the local and the target device cursor. The Video Viewer window supports either a 3- or 5-button mouse.

The SwitchView IP 1020 remote access device on-board web interface software uses a Java-based program to display the Video Viewer window. The SwitchView IP 1020 remote access device OBWI automatically downloads and installs the Video Viewer the first time it is opened.

NOTE: The SwitchView IP 1020 remote access device on-board web interface does not install the Java Resource Engine (JRE). The JRE is available as a free download from http://www.sun.com for PC users and from http://www.apple.com for Mac users. When in IPv4 mode, Java 1.5 or later is required. When in IPv6 mode, Java 1.6 or later is required. Currently, MAC operating systems only support Java 1.5, so users with MAC operating systems cannot yet operate in IPv6 mode.

NOTE: The SwitchView IP 1020 remote access device on-board web interface uses system memory to store and display images within Video Viewer windows. Each opened Video Viewer window requires additional system memory:

- An 8-bit color setting on the client PC requires 1.4 MB of memory per Video Viewer window.
- A 16-bit color setting requires 2.4 MB and a 32-bit color setting requires 6.8 MB.

If the device you are attempting to access is currently being viewed by another user, you will be prompted to preempt the other users if your preemption level is equal to or greater than theirs. An appliance administrator can also disconnect an active user via the Active Session page.

Launching a KVM Session

NOTE: When using a non-proxied connection, video performance over a slower network connection may be less than optimal. Since certain color settings (such as Grayscale) use less network bandwidth than others (such as Best Color), changing the color settings can increase video performance. For optimal video performance over a slower network connection, Avocent recommends a color setting such as Grayscale/Best Compression or Low Color/High Compression. See *1024 x 768 768 x 576 960 x 720 704 x 528 896 x 672 640 x 480 832 x 624* on page 32 for more information.

NOTE: If a user connects to a target device with a higher screen resolution than the local computer, the Video Viewer window will display a portion of the target device screen, with scroll bars for viewing the remainder of the screen. The user may view the entire screen by adjusting the resolution on the target device, the local computer or both.

To launch a KVM session from the SwitchView IP 1020 Explorer window:

1. Click on a device listed on the Target Devices screen to open the unit overview window.
2. Click the *KVM Session* link to open the Video Viewer in a new window.

Session time-out

A remote session can time-out when no activity occurs in a Session window for a specified time. The session time-out value can be configured in the Appliance KVM Session Settings window. The specified time-out value will be used the next time the switch on-board web interface is accessed.

To enable, disable or configure the session time-out:

1. In the side menu, select *Unit Views - Appliance - Appliance Settings - Sessions - KVM Settings.*
2. Select the desired setting for the *Enable Activity Timeout* box.
3. If necessary, select the time limit for the inactivity time-out.

Video Viewer Window Features

Figure 4.1 shows the Video Viewer window areas. Descriptions follow in Table 4.1.

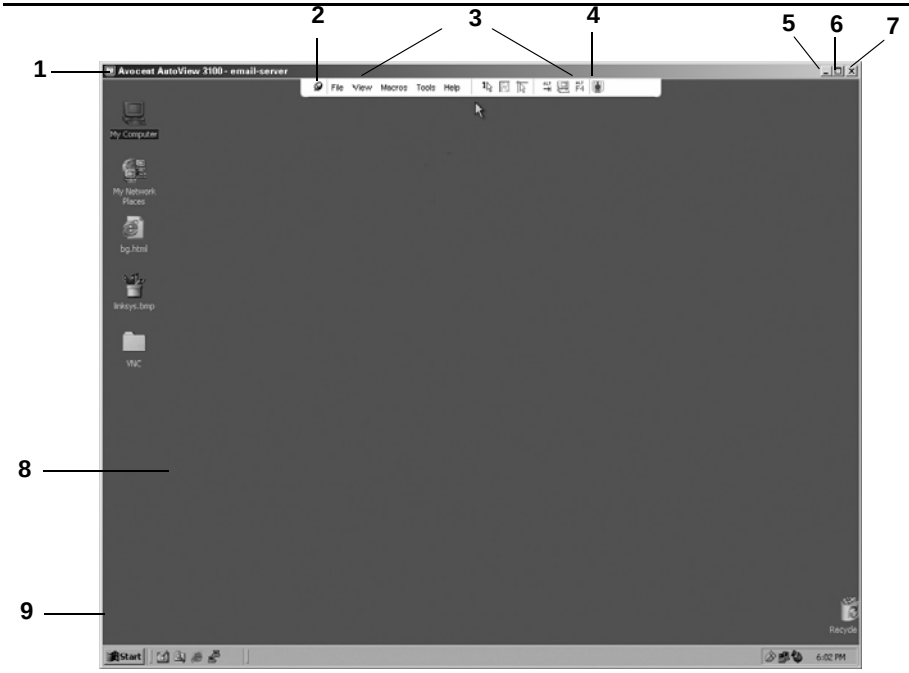


Figure 4.1: Video Viewer Window (Normal Window Mode)

Table 4.1: Descriptions for Figure 5.1

Number	Description
1	Title Bar: Displays the name of the server being viewed. When in Full Screen mode, the title bar disappears and the server name appears between the menu and toolbar.
2	Thumbtack: Locks the display of the menu and toolbar so that it is visible at all times.
3	Menu and toolbar: Enables you to access many of the features in the Video Viewer window. The menu and toolbar is in a show/hide state if the thumbtack has not been used. Place your cursor over the toolbar to display the menu and toolbar. Up to ten commands and/or macro group buttons can be displayed on the toolbar. By default, the Single Cursor Mode, Refresh, Automatic Video Adjust and Align Local Cursor buttons appear on the toolbar. For more information, see *Changing the toolbar* on page 30 and *Using Macros* on page 38.
4	Macro buttons: Commonly used keyboard sequences that can be sent to the target device.
5	Minimize button: Minimizes the display of the Video Viewer window into the task bar at the bottom of the local computer.
6	Maximize button: Changes the window to Full Screen mode, which expands the accessed device desktop to fill the entire screen. Expanding the window causes the following to occur: • The title bar disappears. • The server name appears between the menu and toolbar. • The Maximize button changes to a Normal Window Mode button and appears on the toolbar. Clicking the button toggles the Video Viewer window to Normal Window mode. • The Close button appears on the toolbar.

Table 4.1: Descriptions for Figure 5.1 (Continued)

Number	Description
7	Close button: Closes the Video Viewer window. **NOTE:** The Close button may not be present for all operating systems.
8	Accessed device desktop: Interacts with your device through this window.
9	Frame: Resizes the Video Viewer window by clicking and holding on the frame.

Changing the toolbar

You can choose the amount of elapsed time before the toolbar hides in the Video Viewer window when it is in show/hide state (that is, not locked in place by the thumbtack).

To specify a toolbar hide time:

1. Select *Tools* - *Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Toolbar* tab.
3. Use the arrow keys to specify the number of elapsed seconds prior to hiding the toolbar.
4. Click *OK* to save your changes and close the dialog box.

Setting the window size

NOTE: The View - Scaling command is not available if the Video Viewer window is in Full Screen mode or to non-primary users of a shared session.

When the SwitchView IP 1020 remote access device on-board web interface is used for the first time, any open Video Viewer windows display at a resolution of 1024 x 768 until the user changes the value. Each Video Viewer window can be set to a different resolution.

The SwitchView IP 1020 remote access device on-board web interface automatically adjusts the display if the window size changes during a session as long as autoscaling is enabled. If the target device resolution changes any time during a session, the display adjusts automatically.

To change the Video Viewer window resolution:

1. Select the *View* - *Scaling* command.
2. Click on the desired resolution.

Adjusting the view

Using menus or task buttons in the Video Viewer window, you can do the following:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable Full Screen mode. When Full Screen mode is enabled, the image adjusts to fit the desktop up to a size of 1024 x 768. If the desktop has a higher resolution, the following occurs:
  - The full-screen image is centered in the desktop, and the areas surrounding the Video Viewer window are black.
  - The menu and toolbar are locked so that they are visible at all times.
- Enable automatic, full or manual scaling of the session image:
  - With full scaling, the desktop window remains fixed and the device image scales to fit the window.
  - With automatic scaling, the desktop window is sized to match the resolution of the server being viewed.
  - With manual scaling, a drop-down menu of supported image scaling resolutions is displayed.
- Change the color depth of the session image.

To align the mouse cursors:

Click the *Align Local Cursor* button in the Video Viewer window toolbar. The local cursor should align with the cursor on the remote device.

NOTE: If cursors drift out of alignment, turn off mouse acceleration in the attached device.

To refresh the screen:

Click the *Refresh Image* button in the Video Viewer window.

-or-

Select *View* - *Refresh* from the Video Viewer window menu.

The digitized video image is completely regenerated.

To enable or disable Full Screen mode:

1. To enable Full Screen mode, click the *Maximize* button.
   -or-
   Select *View* - *Full Screen* from the Video Viewer window menu.

   The desktop window disappears and only the accessed device desktop is visible. The screen resizes up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar appears.

   -or-

2. To disable Full Screen mode, click the *Full Screen Mode* button on the floating toolbar to return to the desktop window.

To enable full or manual scaling:

To enable full scaling, select *View - Scaling* from the Video Viewer window menu. The device image scales automatically to the resolution of the server being viewed.

-or-

To enable manual scaling, select *View - Scaling* from the Video Viewer window menu. Choose the dimension to scale the window. Available manual scaling sizes are as follows:

1024 x 768	768 x 576
960 x 720	704 x 528
896 x 672	640 x 480
832 x 624	

Adjusting color depth

The Dambrackas Video Compression® (DVC) algorithm enables users to adjust the number of viewable colors in a remote session window. You can choose to display more colors for the best fidelity or fewer colors to reduce the volume of data transferred on the network.

Video Viewer windows can be viewed using the Best Color Available (slower updates), Best Compression (fastest updates), a combination of Best Color and Best Compression or in Grayscale.

You can specify the color depths of individual ports and channels by selecting the *View - Color* command in a remote session window.

Additional video adjustment

Generally, the Video Viewer window automatic adjustment features optimize the video for the best possible view. However, users can fine-tune the video with the help of Avocent Technical Support by selecting the *Tools - Manual Video Adjust* command in the Video Viewer window menu or clicking the *Manual Video Adjust* button. This displays the Manual Video Adjust dialog box.

Users can also verify the level of packets per second required to support a static screen by observing the packet rate located in the lower left-hand corner of the dialog box.

To manually adjust the video quality of the window:

NOTE: The following video adjustments should be made only on the advice and with the help of Avocent Technical Support.

1. Select *Tools - Manual Video Adjust* from the Video Viewer window menu.
   -or-
   Click the *Manual Video Adjust* button.

   The Manual Video Adjust dialog box appears. Figure 4.2 shows the dialog box, and descriptions follow in Table 4.2.

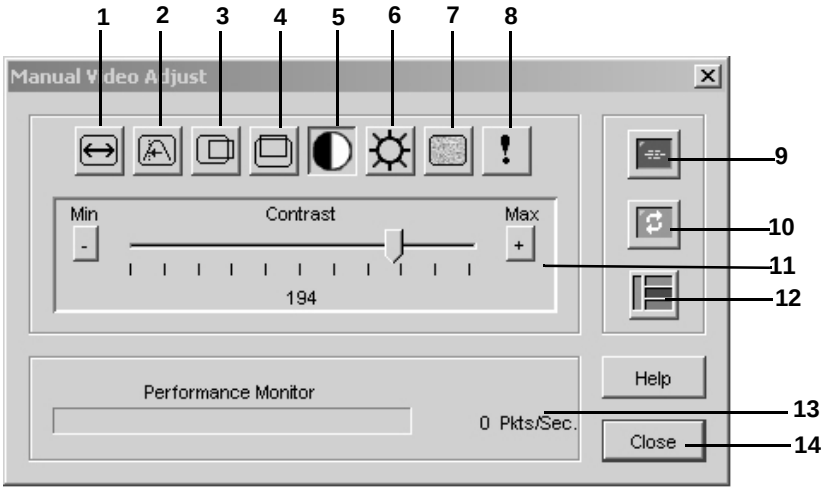


Figure 4.2: Manual Video Adjust Dialog Box

Table 4.2: Descriptions for Figure 5.2

Number	Description	Number	Description
1	Image Capture Width	**8**	Pixel Noise Threshold
2	Pixel Sampling/Fine Adjust	**9**	Automatic Video Adjustment
3	Image Capture Horizontal Position	**10**	Refresh Image
4	Image Capture Vertical Position	**11**	Adjustment bar
5	Contrast	**12**	Video Test Pattern
6	Brightness	**13**	Performance Monitor
7	Block Noise Threshold	**14**	Close button

2. Click the icon corresponding to the feature you wish to adjust.
3. Move the Contrast slider bar and then fine-tune the setting by clicking the *Min* (-) or *Max* (+) buttons to adjust the parameter for each icon pressed. The adjustments display immediately in the Video Viewer window.
4. When finished, click *Close* to exit the Manual Video Adjust dialog box.

Target video settings

The Image Capture Width, Pixel Sampling/Fine Adjust, Image Capture Horizontal Position and Image Capture Vertical Position adjustments affect how the target video is captured and digitized and are seldom changed.

The image capture parameters are automatically changed by the Automatic Adjustment function. A special image is required on the target in order to make accurate adjustments independently.

Contrast and brightness

If the image in the Video Viewer window is too dark or too light, select *Tools - Automatic Video Adjust* or click the *Automatic Video Adjust* button. This command is also available in the Video Adjustments dialog box. In most cases, this corrects video issues.

When clicking *Auto Adjust* several times does not set the contrast and brightness as desired, adjusting the contrast and brightness manually can help. Increase the brightness. Do not go more than 10 increments before moving the contrast. Generally, the contrast should be moved very little.

Detection thresholds

In some cases, noise in the video transmission keeps the packets/sec count up, which is indicated by little dots changing in the area of the cursor when it is moved. Varying the threshold values may result in “quieter” screens and can improve cursor tracking.

You can modify Noise Threshold and Priority Threshold values if you are using standard video compression. You can also modify Block Noise Threshold and Pixel Noise Threshold values. You can restore default threshold values by clicking *Auto Adjust Video*.

Block Noise Threshold and Pixel Noise Threshold

The Block Noise Threshold and Pixel Noise Threshold values set the minimum color levels in terms of changed video blocks and pixels per thousand that are allowed.

- The Block Noise Threshold sets the minimum color change that occurs in a single video block. Increasing the value reduces the network bandwidth. Decreasing the value makes the size of these artifacts smaller.
- The Pixel Noise Threshold sets the minimum color change in a single pixel. Decreasing the value reduces the number of low-contrast artifacts, but increases network bandwidth.

See *Adjusting the view* on page 30 for information about changing the color depth.

Automatic video adjustment

In most cases, you do not need to alter the Video Settings from the default. The system automatically adjusts and uses the optimal video parameters. The SwitchView IP 1020 remote access device on-board web interface performs best when the video parameters are set such that no (0) video packets are transmitted for a static screen.

You can easily adjust your video parameters to ideal settings by clicking on the *Auto Adjust Video* button in the Manual Video Adjust dialog box.

NOTE: You can also select *Tools - Automatic Video Adjust* from the Video Viewer window menu or click the *Automatic Video Adjust* toolbar icon to automatically adjust the video.

Refresh Image

Clicking the *Refresh Image* button in the Manual Video Adjust dialog box completely regenerates the digitized video image.

NOTE: You can also select *View - Refresh* from the Video Viewer window menu to refresh the image.

Video Test Pattern

Clicking the *Video Test Pattern* button in the Manual Video Adjust dialog box toggles a display of a video test pattern. Click the *Video Test Pattern* button again to toggle back to a normal video image.

Adjusting mouse options

The Video Viewer window mouse options affect cursor type, Cursor mode, scaling, alignment and resetting. Mouse settings are device-specific; that is, they may be set differently for each device.

NOTE: If the device does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the device will have to be rebooted.

Cursor type

The Video Viewer window offers five appearance choices for the local mouse cursor. You can also choose no cursor or the default cursor.

In Single Cursor mode, the display of the local (second) cursor in the Video Viewer window turns off and only the target device mouse pointer is visible. The only mouse movements that appear are those of the target device remote cursor. Use Single Cursor mode when there is no need for a local cursor. Figure 4.3 shows both the Remote Cursor and the Local Cursor displayed in the Video Viewer window.

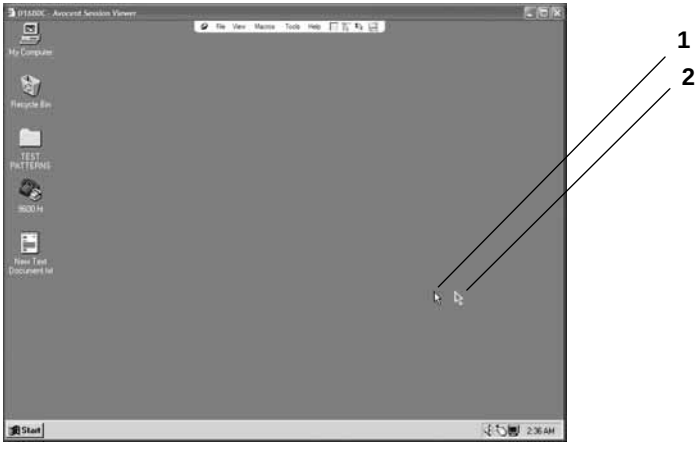


Figure 4.3: Video Viewer Window with Local and Remote Cursors Displayed

Table 4.3: Descriptions for Figure 5.3

Number	Description
1	Remote Cursor
2	Local Cursor

The Cursor mode status of the Video Viewer window displays in the title bar, including the keystroke that will exit Single Cursor mode. You can define the keystroke that will exit Single Cursor mode in the Session Options dialog box.

NOTE: When using a device that captures keystrokes before they reach the client, you should avoid using those keys to restore the mouse pointer.

To enter Single Cursor mode:

Select *Tools - Single Cursor Mode* from the Video Viewer window menu.

-or-

Click the *Single Cursor Mode* button.

The local cursor does not appear and all movements are relative to the target device.

To select a key for exiting Single Cursor mode:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. Select a terminating keystroke from the drop-down menu in the Single Cursor mode area.
4. Click *OK* to save settings.

When you enable Single Cursor mode, you can press the specified key to return to Regular Desktop mode.

To exit Single Cursor mode:

Press the key on the keyboard that is identified in the title bar.

To change the mouse cursor setting:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

The Session Options dialog box appears.

2. Click the *Mouse* tab.
3. Select a mouse cursor type in the Local Cursor panel.
4. Click *OK* to save settings.

Mouse scaling

Some earlier versions of Linux did not support adjustable mouse accelerations. For installations that must support these earlier versions, you can choose among three preconfigured mouse scaling options or set your own custom scaling. The preconfigured settings are Default (1:1), High (2:1) or Low (1:2):

- In a 1:1 scaling ratio, every mouse movement on the desktop window sends an equivalent mouse movement to the server.
- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.
- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *Mouse* tab.
3. To use one of the preconfigured settings, check the appropriate radio button.
   -or-
   To set custom scaling:
   a. Click the *Custom* radio button to enable the X and Y fields.
   b. Type a scaling value in the X and Y fields. For every mouse input, the mouse movements are multiplied by the respective X and Y scaling factors. Valid input range is 0.25-3.00.

Vendor-specific video settings

Video settings vary significantly among manufacturers. Avocent maintains an online database of optimized video settings for various video cards, particularly Sun-specific ones. This information can be obtained from Avocent's online knowledge base or by calling Avocent technical support.

Mouse alignment and synchronization

Because the SwitchView IP 1020 remote access device on-board web interface cannot get constant feedback from the mouse, there are times when the mouse on the SwitchView IP 1020 remote access device may lose sync with the mouse on the host system. If your mouse or keyboard no longer responds properly, you can align the mouse to re-establish proper tracking.

Alignment causes the local cursor to align with the remote server's cursor. Resetting causes a simulation of a mouse and keyboard reconnect as if you had disconnected and reconnected them.

To realign the mouse:

Click the *Align Local Cursor* button in the Video Viewer window toolbar.

Using Keyboard Pass-through

Keystrokes that a user enters when using a Video Viewer window may be interpreted in two ways, depending on the Screen mode of the Video Viewer window.

- If a Video Viewer window is in Full Screen mode, all keystrokes and keyboard combinations except **Ctrl-Alt-Del** are sent to the remote server being viewed.
- If a Video Viewer window is in Regular Desktop mode, Keyboard Pass-through mode can be used to control whether the remote server or local computer recognizes certain keystrokes or keystroke combinations.

Keyboard pass-through must be specified using the Session Options dialog box. When enabled, keyboard pass-through sends all keystrokes and keystroke combinations except **Ctrl-Alt-Del** to the remote server being viewed when the Video Viewer window is active. When the local desktop is active, keystrokes and keystroke combinations entered by the user affect the local computer.

NOTE: The **Ctrl-Alt-Delete** keyboard combination can be sent only to a remote server by using a macro.

NOTE: The Japanese keyboard **ALT-Han/Zen** keystroke combination is always sent to a remote server regardless of the Screen mode or keyboard pass-through setting.

To specify keyboard pass-through:

1. Select *Tools - Session Options* from the Video Viewer window menu.
   -or-
   Click the *Session Options* button.

   The Session Options dialog box appears.
2. Click the *General* tab.
3. Select *Pass-through all keystrokes in regular window mode*.
4. Click *OK* to save setting.

Using Macros

The SwitchView IP 1020 remote access device on-board web interface comes pre-configured with macros for the Windows and the Sun platforms.

To send a macro:

Select *Macros - <desired macro>* from the Video Viewer window menu.

-or-

Select the desired macro from the buttons available on the Video Viewer menu.

Saving the View

You can save the display of a Video Viewer either to a file or to the clipboard for pasting into a word processor or other program.

To capture the Video Viewer window to a file:

1. Select *File - Capture to File* from the Video Viewer window menu.
   -or-
   Click the *Capture to File* button.

   The Save As dialog box appears.
2. Enter a filename and choose a location to save the file.
3. Click *Save* to save the display to a file.

To capture the Video Viewer window to your clipboard:

Select *File - Capture to Clipboard* from the Video Viewer window menu.

-or-

Click the *Capture to Clipboard* button.

The image data is saved to the clipboard.

Closing a Video Viewer Window Session

To close a Video Viewer window session:

Select *File - Exit* from the Video Viewer window.

APPENDICES

Appendix A: Flash Upgrades

The SwitchView IP 1020 remote access device Flash upgrade feature allows you to update your appliance with the latest firmware available.

After the Flash memory is reprogrammed with the upgrade, the SwitchView IP 1020 remote access device performs a soft reset, which terminates all IQ module sessions. A target device experiencing an IQ module firmware update may not display, or may display as disconnected. The target device will appear normally when the Flash update is completed.

CAUTION: Disconnecting or cycling power to the SwitchView IP 1020 device during an update may render the device inoperable and require the SwitchView IP 1020 device to be reprogrammed using the recovery procedure.

To update the SwitchView IP 1020 remote access device firmware:

1. Visit http://www.avocent.com/support and download the latest Flash firmware from Avocent. Save the Flash update file to the appropriate directory on a computer that can access the SwitchView IP 1020 remote access device.
2. If the SwitchView IP 1020 remote access device is not on, turn it on now. After approximately one minute, proceed to login.
3. Select *Firmware Management* to display the current version of your firmware on the Firmware Management menu.
4. Click the *Upgrade Firmware* button.
5. Use the browser to find the appropriate directory and filename.
6. Click the *Upgrade* button.
7. The SwitchView IP 1020 remote access device begins the Flash update process. On-screen indicators display the update progress. When the upload is complete, the SwitchView IP 1020 remote access device resets and updates the internal subsystems.
8. Once the update is complete, the login screen will appear.

NOTE: If the green LED on the back panel of the device blinks continuously, the device is in recovery mode.

To recover a Flash update:

NOTE: If you do not have a TFTP server, you can find several shareware and freeware programs on the Internet that you can download and install.

1. Visit http://www.avocent.com/support and download the latest Flash firmware from Avocent. Save the Flash update file to the appropriate directory on the TFTP server.
2. Use the server IP address 192.168.1 to set up the TFTP server.
3. Rename the downloaded file name to svip1020.fl and place it into the TFTP root directory of the TFTP server.
4. Make sure the SwitchView IP 1020 device is powered.

The recovery should start automatically.

Appendix B: Technical Specifications

Table B.1: SwitchView IP 1020 Remote Access Device Product Specifications

Server Ports	
Number	1
Type	PS/2, USB
Connectors	PS/2, USB, VGA
Sync Types	Separate horizontal and vertical
Plug and Play	DDC2B
Video Resolution	640 x 480 @ 60 Hz 800 x 600 @ 75 Hz 960 x 700 @ 75 Hz 1024 x 768 @ 75 Hz 1280 x 1024 @ 75 Hz (Remote port maximum)
Supported Cabling	CPS2-6A cable, 6 feet
Dimensions	
Height x Width x Depth	1.06 in x 8.19 in x 5.25 in (2.70 cm x 20.80 cm x 13.34 cm)
Weight (without cables)	1.5 lbs (0.68 kg) without cables
Network Connection	
Number	1
Type	10/100/1000 Ethernet
Connector	RJ-45
Local Port	
Number	1
Type	PS/2, VGA
Power Consumption	5 W
Operating Voltage	external 5 V DC power @ 2.0 A
AC-input Power	10.5 W maximum (120 V, 60 Hz)
AC-input Range	100 - 240 VAC

Table B.1: SwitchView IP 1020 Remote Access Device Product Specifications (Continued)

AC Frequency	50 - 60 Hz autosensing
AC-input Current Rating	0.5 A
AC-input Cable	6 ft, 2 conductor, 18 AWG
Ambient Atmospheric Condition Ratings	
Humidity	5 to 95% noncondensing (operating/storage)
Temperature	0° to 40° Celsius (32° to 104° degrees Farenheit) operating -30° to 70° Celsius (-22° to 149° Farenheit) nonoperating
Safety and EMC Standards Approvals and Markings	UL, FCC, cUL, ICES-003, CE, GS, VCCI, MIC, C-Tick Safety certifications and EMC certifications for this product are obtained under one or more of the following designations: CMN (Certification Model Number), MPN (Manufacturer's Part Number) or Sales Level Model designation. The designation that is referenced in the EMC and/or safety reports and certificates are printed on the label applied to this product.

Appendix C: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard can be emulated by key press sequences on a PS/2 keyboard. To enable Sun Advanced Key Emulation mode and use these keys, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key. The *Scroll Lock* LED blinks. Use the indicated keys in Table C.1 as you would use the advanced keys on a Sun keyboard.

Table C.1: Sun Key Emulation

Sun Key (US)	PS/2 Key to Enable Sun Key Emulation
Compose	Application(1)
Compose	keypad
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad /
Vol.+	keypad +
Vol.-	keypad -
Command (left)(2)	F12
Command (left)(2)	Win (GUI) left (1)
Command (right)(2)	Win (GUI) right (1)

(1)Windows 95 104-key keyboard.
(2)The Command key is the Sun Meta (diamond) key.

For example: For **Stop + A**, press and hold **Ctrl+Shift+Alt** and press Scroll Lock, then **F1 + A**.

These key combinations will work with the serial USB IQ module (if your Sun system comes with a USB port) as well as the Sun VSN and WSN IQ modules. With the exception of **F12**, these key combinations are not recognized by Microsoft Windows. Using **F12** performs a Windows key press.

When finished, press and hold **Ctrl+Shift+Alt** and then press the **Scroll Lock** key to toggle Sun Advanced Key Emulation mode off.

Special considerations for Japanese Sun USB and Korean Sun USB keyboards (USB IQ modules only)

Japanese Sun USB and Korean Sun USB keyboards assign usage IDs for certain keys that differ from standard USB usage IDs. If USB IQ modules are attached to your Sun servers, the Han/Zen and Katakana/Hiragana keys on Japanese Sun USB keyboards and Hangul and Hanja keys on Korean Sun USB keyboards must be accessed using alternate keystrokes.

Due to these keyboard-specific differences, keyboard mapping inconsistencies may be encountered when switching between target devices using Sun VSN and WSN IQ modules and target devices using USB IQ modules. These keys function normally if your Sun servers are attached to the SwitchView IP 1020 remote access device using a VSN or WSN IQ module.

Table C.2 lists the keyboard mapping that will take place when a USB IQ module is used in this setting.

Table C.2: PS/2-to-USB Keyboard Mappings

PS/2 Keyboard	USB Usage ID	Sun USB Keyboard	Korean Sun USB Keyboard	Japanese Sun USB Keyboard
Right-Alt	0xE6	AltGraph	Hangul	Katakana/Hiragana
Windows Application	0x65	Compose	Hanja	Compose
Hangul	0x90	N/A	N/A	N/A
Hanja	0x91	N/A	N/A	N/A
Katakana/Hiragana	0x88	N/A	N/A	Han/Zen
Han/Zen	0x35	` ~	` ~	N/A

Appendix D: Reset to Factory Defaults

To reset your SwitchView IP 1020 remote access device to the factory defaults:

1. Locate the small hole on the right side of the SwitchView IP 1020 device.
2. Insert a pin to depress the reset switch and hold for three (3) seconds.

NOTE: This will reboot the SwitchView IP 1020 remote access device, and all connections will be lost.

3. The blue LED on the front panel of the SwitchView IP 1020 device will blink twice to indicate that the device is being reprogrammed.
4. Log in to the device again once it has been reset to the factory defaults.

NOTE: The default username is Admin with no password.

Appendix E: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

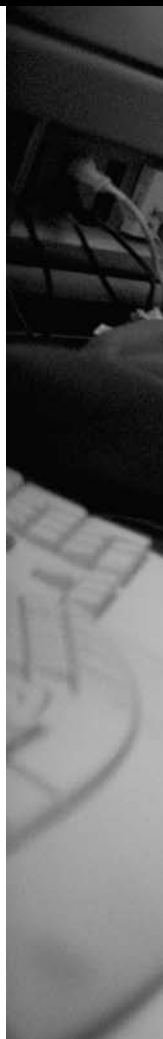
1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

Avocent

The Power of Being There®

For Technical Support:

www.avocent.com/support



590-538-501D